UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/736,445	12/15/2003	Wenge Chen	1033-LB1029	3091

60533 7590 02/19/2008

TOLER LAW GROUP
8500 BLUFFSTONE COVE
SUITE A201
AUSTIN, TX 78759

EXAMINER	
AHMED, SALMAN	

ART UNIT	PAPER NUMBER
2619	

MAIL DATE	DELIVERY MODE
02/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/736,445	CHEN ET AL.	
	Examiner	Art Unit	
	Salman Ahmed	2619	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/29/2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12/15/2003 and 5/28/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-26 are pending.

Claims 1-26 are rejected.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 10, 11, 13, 15, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan et al. (US PAT PUB 2002/0191541, hereinafter Buchanan).

In regards to claim 10, Buchanan teaches *a method of provisioning a virtual private network service, the method comprising: providing a set of rules regarding assignment of route targets for each of a plurality of virtual private networks* (section 0029, 0031 and 0076, A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create the topological relationship (*providing a set of rules)* between different sites. Route Targets may be used to describe the topology of a VPN, for example the permitted combination (*a set of rules)* of sites which may communicate securely over the VPN. A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. This prevents (*a set of rules)* communication between sites which have no VPN in common); *configuring provider edge routers of a backbone network* (Figure 1, backbone network 120 and section 0029, 0031 and 0076, A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create (*configure*) the topological relationship between different sites. Any route associated with a Route Target T is distributed to every Provider Edge (PE) router that has a VRF associated with Route Target T. When such a route is received by a PE router, it is eligible to be installed on those of the PE's VRFs which are associated with Route Target T); *configuring customer edge routers, each of the customer edge routers having a relationship link to at least one of the provider edge routers; assigning route targets to each of the customer edge routers based on topology requirements of a backbone network and based on the set of rules* (Figure 1, backbone network 120 and sections 0023, 0029, 0031, 0044, 0046 and 0076,

A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create (*configure*) the topological relationship between different sites. It is a unique aspect of Border Gateway Protocol 4 (BGP) and Multi-protocol Label Switching (MPLS) VPNs that the VPN connectivity is provided by a dedicated provider edge-customer edge (PE-CE) peering relation combined with a shared packet-switched network operable to deliver packetized data between nodes/sites. Routing information acceptance is preferably based on the Route Targets (RTs) in the advertisement from the route reflectors. The accepted routes are preferably advertised to the CE router. If desired, the accepted routes may also be installed on the PE to CE user ports. The routes accepted by the PE-CE peering protocol are preferably advertised to the CE and installed on the corresponding network processor); *and configuring each of the VRFs and RTs on the corresponding provider edge routers to form a logical topology* (section 0029, 031 and 0076 A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create (*configure*) the topological relationship between different sites. Route Targets may be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. Every VRF is associated with one or more Route Target attributes. Any route associated with a Route Target T is distributed to every Provider Edge (PE) router that has a VRF associated with Route Target T. When such a route is received by a PE router, it is eligible to be installed on those of the PE's VRFs which are

associated with Route Target T). Buchanan teaches *grouping a set of route targets from the plurality of route targets* (Figure 4 and section 0029, Route targets are grouped into Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target, Secondary Route Target).

Buchanan does not explicitly teach *removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same.*

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with steps of *removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same.* The motivation is that by such method duplicate Route Target may be avoided, thus reducing system overhead and facilitating efficient use of network resources, further improving storage process by preventing duplicate storage of same data in the storage device, thereby reducing the storage space.

In regards to claim 11, Buchanan anticipates adding an additional CE to one of the plurality of virtual private networks to form a modified logical topology (section 0039, utilizing the user interface of the present invention a VPN, a customer, and/or a site may be added by right clicking on a customer entry and making the appropriate selection from a pop-up menu. This inherently modifies the existing topology).

In regards to claim 13, Buchanan anticipates the modified logical topology has a new VPN with respect to the logical topology (section 0039, utilizing the user interface

of the present invention a VPN, a customer, and/or a site may be added by right clicking on a customer entry and making the appropriate selection from a pop-up menu. This inherently modifies the existing topology and creates a new VPN which is topologically different from the prior VPN).

In regards to claim 15, Buchanan teaches communicating the logical topology to a remote computer system (section 0031, MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database, and transmits it to the appropriate routers, switches and/or devices of the network) wherein the logical topology includes a modified topology type, the modified topology type changed from mesh to a full Hub and Spoke arrangement (section 0112).

Buchanan teaches the modified topology type changed from mesh to a full Hub and Spoke arrangement but does not explicitly teach the modified topology type changed from Hub and Spoke to a full mesh arrangement. It is within the appreciation or one of ordinary skilled in the art to modify Buchanan's teaching with steps of modified topology type being changed from Hub and Spoke to a full mesh arrangement; as depending on network requirement, available resources, estimated traffic etc. a network topology can be modified from Hub and Spoke to a full mesh arrangement or vice versa; enabling the modified network to successfully accommodate changing requirements.

In regards to claim 18, Buchanan teaches *the high level description of the topology of the network comprises a plurality of data entries, a first set of the data entries identifying customer edge (CE) routers* (section 0040, The site interface details

window preferably contains one or more of the following data fields to be filled by the provisioning operator: Name, interface IP Address, Subnet Mask, Route Distinguisher, and/or the like), *a second set of data entries identifying provider edge routers* (service provider) *corresponding to each of the customer edge routers* (section 0035, Preferably when configuring VPNs, VPN tree 210 includes one or more of the following data categories: service provider, customers, sites (customer edge routers), site interfaces, VPNs, VPN components, VPN interfaces, and/or the like), *a third set of the data entries identifying a topology type for each of the virtual private networks* (sections 0043, A VPN component may be added to an existing VPN entry by right clicking on a VPN entry and making the appropriate selection from the pop-up menu. The details for the VPN component may then be filled in. The VPN component details window preferably contains one or more of the following data fields to be filled by the provisioning operator: Name, Component Number, Component Topology (topology type), Primary Route Target, Secondary Route Target, and/or the like).

In regards to claim 19, Buchanan teaches *the network element is a VRF component within a data router* (section 0029, Route Targets may be used to describe the topology of a VPN, for example A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. Every VRF is associated with one or more Route Target attributes) *and wherein the topology type is selected from full mesh, hub and spoke topology types* (section 0011, It is yet another technical advantage of an exemplary embodiment provisioning system that it is capable of

understanding and using VPN topology for each VPN to facilitate construction of rules, wherein the mesh and hub-spoke VPN components translate to a specific set of rules constraining routing distribution and therefore communications paths to only those other sites with permitted communication relationships as opposed to all sites reachable via an underlying shared packet switched network) *and central service* (section 0053, A hub-spoke arrangement may be useful in the following cases: central services site, firewall site, and/or the like. A central services site services the spoke and thus, there is no requirement for inter-spoke communication).

4. Claims 8, 9 and 21-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan et al. (US PAT PUB 2002/0191541, hereinafter Buchanan) in view of Li et al. (US PAT PUB 2004/0037275, hereinafter Li).

In regards to claim 8, Buchanan teaches a *computer network operations system* (section 0044, PE node) *comprising: a terminal having a display portion* (FIG. 2 screen display of MCS 201); *a data input device to receive input from a user* (section 0039, Utilizing the user interface of the present invention a VPN, a customer, and/or a site may be added by right clicking *(data input device mouse)* on a customer entry and making the appropriate selection from a pop-up menu); *a computer system* (a Management and Control System (MCS) 201 (FIG. 2)) *having a memory* (section 0031, (MCS) 201 a client-server based software system has inherently a memory associated with it) *and a processor* (section 0031, (MCS) 201 a client-server based software system has inherently a processor associated with it), *the computer system* (a

Management and Control System (MCS) 201 (FIG. 2)) *coupled to the terminal and to the data input device; wherein the display portion of the terminal provides an input screen having a data format configured to prompt the user to provide high-level network topology data via the data input device, the high-level network topology data including virtual private network information with respect to a backbone data network* (sections 0040-0041, a site interface may be added by right clicking on a site entry and making the appropriate selection from the pop-up menu. The details for the site interface can then be filled in. When a site interface is added to a VPN component on the graphical view, the corresponding site graphic is added to the graphical view. A corresponding VPN interface is created in VPN tree 210 under the component); *wherein the computer system converts the high-level network topology data into a set of route targets* (Figure 4 a set route targets provisioned are Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target, Secondary Route Target. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN) *to be assigned to virtual routing and forwarding elements,* (sections 0029, 0076 and 0031, Route Targets are be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. MCS 201 preferably automatically generates a routing policy table for each site of the VPN based at least in part on the provisioning operator's intent as specified graphically by the provisioning operator utilizing user interface 200. A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create the topological

relationship between different sites. User interface 200 preferably also allows the provisioning operator to graphically set-up routing relationships between the different sites. However, user interface 200 only allows routing relationships to be set-up based on the constraints of the underlying topology. Thus, by being aware of the rules corresponding to the topology, MCS 201 allows provisioning of routing relationships based on the topology. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN) *the set of route targets (*Figure 4 set of route targets are Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target, Secondary Route Target) *stored in the memory* (sections 0029, 0076 and 0031Route Targets are be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database).

In regards to claim 21, Buchanan teaches *a system to monitor a backbone network, the system comprising: a terminal having a display portion* (FIG. 2 screen display of the MCS 201); *a data input device to receive input from a user* (section 0039, Utilizing the user interface of the present invention a VPN, a customer, and/or a site may be added by right clicking (*a data input device mouse)* on a customer entry and making the appropriate selection from a pop-up menu); *a computer system* (a Management and Control System (MCS) 201 (FIG. 2)) *having a memory and a*

processor (section 0031, (MCS) 201 a client-server based software system has inherently a memory and a processor associated with it), *the computer system* (a Management and Control System (MCS) 201 (FIG. 2)) *coupled to the terminal and to the data input device; wherein the display portion of the terminal provides an input screen having a data format configured to prompt the user to provide high-level network topology data via the data input device, the backbone network* (Figure 1, backbone network 120) *including a plurality of CEs, a plurality of PEs, a plurality of virtual routing and forwarding components, a plurality of route targets, and a plurality of virtual private networks* (sections 0029 and 0031, A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create the topological relationship between different sites. User interface 200 preferably also allows the provisioning operator to graphically set-up routing relationships between the different sites. However, user interface 200 only allows routing relationships to be set-up based on the constraints of the underlying topology. Thus, by being aware of the rules corresponding to the topology, MCS 201 allows provisioning of routing relationships based on the topology. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN. Route Targets may be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. Every VRF is associated with one or more Route Target attributes) *and wherein the high level network topology data*

identifies the CEs, the PEs within each of the virtual private networks (section 0023, It is a unique aspect of Border Gateway Protocol 4 (BGP) and Multi-protocol Label Switching (MPLS) VPNs that the VPN connectivity is provided by a dedicated provider edge-customer edge (PE-CE) peering relation (*high level network topology data)* combined with a shared packet-switched network operable to deliver packetized data between nodes/sites); *and wherein the computer system includes a set of rules to convert the high-level network topology data into a set of route targets to be assigned to virtual routing and forwarding (VRF) elements* (Figure 4 a set of route targets are Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target, Secondary Route Target; sections 0029, 0076 and 0031, Route Targets are be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. MCS 201 preferably automatically generates a routing policy table for each site of the VPN based at least in part on the provisioning operator's intent as specified graphically by the provisioning operator utilizing user interface 200. A user interface 200 associated with MCS 201 allows a provisioning operator to graphically create the topological relationship between different sites. User interface 200 preferably also allows the provisioning operator to graphically set-up routing relationships between the different sites. However, user interface 200 only allows routing relationships to be set-up based on the constraints of the underlying topology. Thus, by being aware of the rules corresponding to the topology, MCS 201 allows provisioning of routing relationships based on the topology. MCS 201 captures the provisioning operator's intent, performs

the desirable validation and translation into routing rules for different sites of the VPN), *the set of route targets stored in the memory* (sections 0029, 0076 and 0031, Route Targets are be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules (*set of route targets)* for different sites of the VPN, stores the information in a database).

In regards to claims 8 and 21, Buchanan does not explicitly teach a virtual routing and forwarding (VRF) element to route target data mapping for each of a plurality of provider edge routers (PEs) and wherein all of the customer edge routers with the same route target (RT) set on one PE share one VRF.

Benjamin in the same field of endeavor teaches a virtual routing and forwarding (VRF) element to route target data mapping for each of a plurality of provider edge routers (PEs) and wherein all of the customer edge routers with the same route target (RT) set on one PE share one VRF (paragraph 0022, figure 2).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with steps of a virtual routing and forwarding (VRF) element to route target data mapping for each of a plurality of provider edge routers (PEs) and wherein all of the customer edge routers with the same route target (RT) set on one PE share one VRF as suggested by Benjamin. The motivation is that such VRF-RT model is used for efficiently and reliably determining VPN topologies,

and element members; thus enabling a simplified method of maintaining and updating topology and routing configuration.

In regards to claim 9, Buchanan teaches the backbone data network is a multi protocol label switching (MPLS) network (section 0005, Accordingly, especially with the introduction of newer technologies, such as Border Gateway Protocol 4 (BGP) and Multi-protocol Label Switching (MPLS), there is a need in the art for a system and method for routing policy provisioning in a network, such as topology constrained routing policy provisioning in a Virtual Private Network (VPN), for example a BGP MPLS VPN).

In regards to claim 22, Buchanan anticipates *the set of rules includes a first set of rules to handle route target to VRF mapping based on a meshed topology and a second set of rules to handle route targets to VRF mapping for a hub and spoke topology* (section 0084, FIG. 5 shows a schematic diagram of an exemplary VPN 500. VPN 500 comprises a hub-spoke VPN component X1 (502) with site S1 (504) as the hub and sites S2 (506), S3 (508), and S4 (510) as the spokes. VPN 500 also comprises a mesh VPN component X2 (512) with sites Si (504) and S5 (514) as members of the mesh) *and a third set of rules to handle route targets to VRF mapping for a central service topology* (section 0053, A hub-spoke arrangement may be useful in the following cases: central services site, firewall site, and/or the like. A central services site services the spoke and thus, there is no requirement for inter-spoke communication. In the case of a firewall site, all the communication between the spokes has to go through the firewall

site, which acts as a hub site. In order to enable firewall operations import and export rule mechanisms may be used).

In regards to claim 23, Buchanan anticipates the second set of rules includes an import rule and an export rule (Figure 4 and section 0079).

In regards to claim 24, Buchanan anticipates the second set of rules applies to two route targets for a particular VRF component (Figure 4, Import Route Target and Export Route Target).

In regards to claim 25, Buchanan anticipates the memory (database) further stores a software program to generate and deploy the set of route targets into a physical network router node (section 0031, Preferably a Management and Control System (MCS) 201 (FIG. 2), which is preferably a client-server based software system, is utilized for topology constrained QoS (Quality of Service) and routing policy provisioning according to the preferred embodiment of the present invention. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database, and transmits (inherently by generating an output file including output data) it to the appropriate routers, switches and/or devices of the network).

In regards to claim 26, Buchanan anticipates the memory (database) further includes a VRF to route target data mapping for each of a plurality of PEs and wherein all the CEs with the same RT set on one PE share one VRF (Figure 4 and sections 0029 and 0063, Route Targets may be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the

VPN. A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. This prevents communication between sites which have no VPN in common. Every VRF is associated with one or more Route Target attributes. Any route associated with a Route Target T is distributed to every Provider Edge (PE) router that has a VRF associated with Route Target T. When such a route is received by a PE router, it is eligible to be installed on those of the PE's VRFs which are associated with Route Target T. Local export rules 308 preferably associate a particular IPv4 route from PE-CE routing protocol with information items, such as RD, RT, SOO, VPN_ID, IPv4 prefix, NextHopInfo, and/or the like).

5. Claims 1, 2, 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan et al. (US PAT PUB 2002/0191541, hereinafter Buchanan) in view of Datta et al. (US PAT 7024472, hereinafter Datta).

In regards to claim 1, Buchanan teaches *an automated method of provisioning a virtual private network* (Figure 1, topology 100), *the method comprising: receiving a high level description of a topology of a network* (section 0031, MCS 201 receives topological relationship between different sites from operator via user interface 200); *applying a set of rules* (section 0031, applying desirable validation and translation) *to the topology of the network to produce a plurality of route targets* (Figure 4 and section 0029, producing plurality of route targets which are Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target,

Secondary Route Target) *associated with virtual private networks* (section 0029, Route Targets are be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN) *to be assigned to the network* (section 0031, thus, by being aware of the rules corresponding to the topology, MCS 201 allows provisioning of routing relationships based on the topology. MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database); *grouping a set of route targets from the plurality of route targets* (Figure 4 and section 0029, Route targets are grouped into Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target, Secondary Route Target) *with respect to each customer equipment node within the network to form a group of route target sets* (Figure 4 Route target sets are group of route targets grouped into Import Route Target, Export Route Target, Remote Export Route Target etc. as well as Table 1 Primary Route Target, Secondary Route Target, abstract and section 0029, enabling graphically defining of relationships between the plurality of sites (*customer equipment node)* of the VPN; and automatically generating at least one routing rule for each site of the VPN based at least in part on the defined relationship. Route Targets are used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN); *removing duplicate route sets from the group of route target sets to form a reduced size of route target sets based on the routes between duplicate route target sets being the same* (section 0062 and 0063, Any routes which are not accepted are discarded, for

example, routes from the same site are typically discarded, i.e. duplicate routes are removed and route target is a part of the route); *assigning each set of route targets in the reduced size set of route targets to a virtual routing and forwarding VRF element and all the CEs with the same RT set on one PE share one VRF* (Figure 4 and sections 0029 and 0063, Route Targets may be used to describe the topology of a VPN, for example the permitted combination of sites which may communicate securely over the VPN. A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. This prevents communication between sites which have no VPN in common. Every VRF is associated with one or more Route Target attributes. Any route associated with a Route Target T is distributed to every Provider Edge (PE) router that has a VRF associated with Route Target T. When such a route is received by a PE router, it is eligible to be installed on those of the PE's VRFs which are associated with Route Target T. Local export rules 308 preferably associate a particular IPv4 route from PE-CE routing protocol with information items, such as RD, RT, SOO, VPN_ID, IPv4 prefix, NextHopInfo, and/or the like); *and generating an output including output data that identifies each of the VRFs* (section 0029, Every VRF is associated with one or more Route Target attributes) *and the associated route targets* (section 0023, The association between routes and RTs is preferably performed via filters or rules) *assigned to each of the VRFs* (section 0031, MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules (*generated information is an output including data)* for different sites of the VPN, stores the information in a

database, and transmits it (*an output including data)* to the appropriate routers, switches and/or devices of the network).

In regards to claim 2, Buchanan teaches communicating the output data to a network element within the network (section 0031, MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database, and transmits it to the appropriate routers, switches and/or devices of the network).

Buchanan does not explicitly teach the information exchange is in a file format as in claim 1 and 2.

Datta in the same field of endeavor teaches information being exchanged in a file format (column 7 lines 13-14, an node receives raw data from the network, a flat file, or database).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with steps of exchanging information in a file format as suggested by Datta. The motivation is that file format data are easy to read by operators, as oppose to machine code type executable files; thus making the network fault diagnostic process easier for the operator as he/she can visually see and read the parameters being exchanged between the entities.

In regards to claims 1 and 2, Buchanan and Datta do not explicitly teach *removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same.*

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan Datta's teaching with steps of *removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same.* The motivation is that by such method duplicate Route Target may be avoided, thus reducing system overhead and facilitating efficient use of network resources, further improving storage process by preventing duplicate storage of same data in the storage device, thereby reducing the storage space.

In regards to claim 5, Buchanan teaches *the high level description of the topology of the network comprises a plurality of data entries, a first set of the data entries identifying customer edge (CE) routers* (section 0040, The site interface details window preferably contains one or more of the following data fields to be filled by the provisioning operator: Name, interface IP Address, Subnet Mask, Route Distinguisher, and/or the like), *a second set of data entries identifying provider edge routers* (service provider) *corresponding to each of the customer edge routers* (section 0035, Preferably when configuring VPNs, VPN tree 210 includes one or more of the following data categories: service provider, customers, sites (*customer edge routers*), site interfaces, VPNs, VPN components, VPN interfaces, and/or the like), *a third set of the data entries identifying a topology type for each of the virtual private networks* (sections 0043, A VPN component may be added to an existing VPN entry by right clicking on a VPN entry and making the appropriate selection from the pop-up menu. The details for the VPN component may then be filled in. The VPN component details window preferably

contains one or more of the following data fields to be filled by the provisioning operator: Name, Component Number, Component Topology (topology type), Primary Route Target, Secondary Route Target, and/or the like).

In regards to claim 6, Buchanan teaches *the network element is a VRF component within a data router* (section 0029, Route Targets may be used to describe the topology of a VPN, for example A Virtual Routing Forwarding (VRF) table associated with a particular site S is populated only with routes that lead to other sites which have at least one VPN in common with site S. Every VRF is associated with one or more Route Target attributes) *and wherein the topology type is selected from full mesh, hub and spoke topology types* (section 0011, It is yet another technical advantage of an exemplary embodiment provisioning system that it is capable of understanding and using VPN topology for each VPN to facilitate construction of rules, wherein the mesh and hub-spoke VPN components translate to a specific set of rules constraining routing distribution and therefore communications paths to only those other sites with permitted communication relationships as opposed to all sites reachable via an underlying shared packet switched network) *and central service* (section 0053, A hub-spoke arrangement may be useful in the following cases: central services site, firewall site, and/or the like. A central services site services the spoke and thus, there is no requirement for inter-spoke communication).

6. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan and Datta as applied to claim 1 above and further in view of Zavgren, Jr. (US PAT 6909696, hereinafter Zavgren).

In regards to claim 3 Buchanan teaches generating an output file including output data (section 0031, MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database, and transmits it to the appropriate routers, switches and/or devices of the network) as described in the rejections of claim 3 above.

Buchanan and Datta do not explicitly teach routers, switches and/or devices of the network having a display.

Zavgren in the same field of endeavor teaches router having a display (column 5 lines 3-5, The system 400 displays the network topology with the actual node positions to an operator via a graphical user interface).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan and Datta's system/method with the teachings of router having a display as suggested by Zavgren. The motivation is that such output helps monitor network topology in a non-intrusive manner and in terms of topology design help in visualizing the construction of the network beforehand for subsequent manipulation by an operator; thus making the network visualization and design process seamless, reliable and non-intrusive.

In regards to claim 4, Buchanan and Datta do not explicitly teach displaying a report based on the output data.

Zavgren in the same field of endeavor teaches displaying a report (a complete record) based on the output data (column 4 lines 60-67 and column 5 lines 3-5, to permit recreation of the network operation, the system 400 collects information from the node databases 250 (i.e., the diaries 310 and the forwarding tables 350) and stores the information in its memory (e.g., main memory 430) [step 510]. From the diary 310 information, the system 400 reconstructs the network operation [step 520]. The system 400 may combine the diary 310 information from each of the nodes and sort it by time to establish a complete record of the network operation. The system 400 may also construct its own forwarding tables using the diary 310 information. The system 400 displays the network topology with the actual node positions to an operator via a graphical user interface).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with the teachings of displaying a report based on the output data as suggested by Zavgren. The motivation is that such output helps monitor network topology in a non-intrusive manner and in terms of topology design help in visualizing the construction of the network beforehand for subsequent manipulation by an operator; thus making the network visualization and design process seamless, reliable and non-intrusive.

7. Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan et al. (US PAT PUB 2002/0191541, hereinafter Buchanan) in view of Zavgren, Jr. (US PAT 6909696, hereinafter Zavgren).

In regards to claim 16 Buchanan teaches generating an output file including output data (section 0031, MCS 201 captures the provisioning operator's intent, performs the desirable validation and translation into routing rules for different sites of the VPN, stores the information in a database, and transmits it to the appropriate routers, switches and/or devices of the network) as described in the rejections of claim 3 above.

Buchanan does not explicitly teach routers, switches and/or devices of the network having a display as in claims 3 and 16.

Zavgren in the same field of endeavor teaches router having a display (column 5 lines 3-5, The system 400 displays the network topology with the actual node positions to an operator via a graphical user interface).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with the teachings of router having a display as suggested by Zavgren. The motivation is that such output helps monitor network topology in a non-intrusive manner and in terms of topology design help in visualizing the construction of the network beforehand for subsequent manipulation by an operator; thus making the network visualization and design process seamless, reliable and non-intrusive.

In regards to claim 17, Buchanan teaches the terminal is an operations terminal of a network management system (Control System (MCS) 201), the network management system tied to the backbone network (Figure 1, topology 100 and section

0031, a Management and Control System (MCS) 201 (FIG. 2), which is preferably a client-server based software system, is utilized for topology routing policy provisioning).

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan and Datta as applied to claim 1 above and further in view of Chang et al. (US PAT PUB 2003/0079043, hereinafter Chang).

In regards to claim 7 Buchanan teaches the network is a multi protocol label switching (MPLS) network (section 0005, Accordingly, especially with the introduction of newer technologies, such as Border Gateway Protocol 4 (BGP) and Multi-protocol Label Switching (MPLS), there is a need in the art for a system and method for routing policy provisioning in a network, such as topology constrained routing policy provisioning in a Virtual Private Network (VPN), for example a BGP MPLS VPN) and wherein the plurality of data entries has a table format and the table entries include the associated provider edge routes (section 0076, FIG. 4 shows an exemplary screen display of routing policy 400 for a site of the network of FIG. 1).

Buchanan and Datta do not explicitly teach the rows are virtual private networks, a set of columns is defined by the customer edge routers.

Chang in the same field of endeavor teaches the rows are virtual private networks, a set of columns are defined by the customer edge routers (Figure 7).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan and Datta's system/method with steps of the rows being a virtual private networks, a set of columns being defined by the customer

edge routers as suggested by Chang. The motivation is that tables having CE, PE and VPN association can be designed in any arbitrary format for optimum performance, depending on system requirement, network topology chosen, number of virtual connection required, data type and various other parameters; thus enabling the network to perform seamlessly and efficiently. Choosing the rows as virtual private networks, columns as customer edge routers, is one arbitrary table design that can be implemented for optimum network performance.

9. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan in view of Chang et al. (US PAT PUB 2003/0079043, hereinafter Chang).

In regards to claim 20 Buchanan teaches the network is a multi protocol label switching (MPLS) network (section 0005, Accordingly, especially with the introduction of newer technologies, such as Border Gateway Protocol 4 (BGP) and Multi-protocol Label Switching (MPLS), there is a need in the art for a system and method for routing policy provisioning in a network, such as topology constrained routing policy provisioning in a Virtual Private Network (VPN), for example a BGP MPLS VPN) and wherein the plurality of data entries has a table format and the table entries include the associated provider edge routes (section 0076, FIG. 4 shows an exemplary screen display of routing policy 400 for a site of the network of FIG. 1).

Buchanan does not explicitly teach the rows are virtual private networks, a set of columns is defined by the customer edge routers.

Chang in the same field of endeavor teaches the rows are virtual private networks, a set of columns are defined by the customer edge routers (Figure 7).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with steps of the rows being a virtual private networks, a set of columns being defined by the customer edge routers as suggested by Chang. The motivation is that tables having CE, PE and VPN association can be designed in any arbitrary format for optimum performance, depending on system requirement, network topology chosen, number of virtual connection required, data type and various other parameters; thus enabling the network to perform seamlessly and efficiently. Choosing the rows as virtual private networks, columns as customer edge routers, is one arbitrary table design that can be implemented for optimum network performance.

10. Claims 12 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buchanan in view of Chu et al. (US PAT PUB 2004/0255028, hereinafter Chu).

In regards to claim 12, Buchanan teaches adding CE to VPN to modify topology (section 0039).

Buchanan does not explicitly teach deleting one of the CEs of one of the plurality of virtual private networks to form a modified logical topology.

Chu in the same field of endeavor teaches deleting one of the CEs of one of the plurality of virtual private networks to form a modified logical topology (page 10, claim 12).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with steps of deleting one of the CEs of one of the plurality of virtual private networks to form a modified logical topology as suggested by Chu. The motivation is that, removing a CE changes the structure of the network and to keep the routing table/rules up-to-date and reliable, topology map is updated as soon as possible; thus enabling seamless routing.

In regards to claim 14, Buchanan does not explicitly teach the modified logical topology has a removed VPN with respect to the logical topology.

Chu in the same field of endeavor teaches the modified logical topology has a removed VPN with respect to the logical topology (page 10, claim 12).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan's teaching with steps of the modified logical topology having a removed VPN with respect to the logical topology as suggested by Chu. The motivation is that, removing a CE changes the structure of the network as well as the existing VPN, and to keep the routing table/rules up-to-date and reliable, topology map is updated as soon as possible with the removed VPN modified to new VPN; thus enabling seamless routing.

Response to Arguments

11. Applicant's arguments, see pages 8-19 of the Remarks section, filed 1/29/2008, with respect to the rejections of the claims have been fully considered.

35 USC 103 rejection of claims 1, 2, 5 and 6:

Applicant argues (page 9 paragraph 2) that Buchanan et al. and Datta et al. do not disclose a method comprising removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same, as recited in claim 1. However, Examiner respectfully disagrees with the Applicant's assertion. Buchanan in view of Datta do indeed teach the cited limitation. Specifically, Buchanan teaches *removing duplicate route sets from the group of route target sets to form a reduced size of route target sets based on the routes between duplicate route target sets being the same* (section 0062 and 0063, Any routes which are not accepted are discarded, for example, routes from the same site are typically discarded, i.e. i.e. duplicate routes are removed and route target is a part of the route). However, Buchanan and Datta do not explicitly teach *removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same.* It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Buchanan Datta's teaching with steps of *removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same.* The motivation is that by such method duplicate Route Target may be avoided, thus reducing system overhead and facilitating efficient use of network resources, further improving storage process by preventing duplicate storage of same data in the storage device, thereby reducing the storage space.

Applicant argues (page 9 paragraph 2) that Datta et al. makes no mention of a method comprising removing duplicate route target sets from the group of route target sets to form a reduced size of route target sets based on the route targets between duplicate route target sets being the same. However, Examiner respectfully disagrees with the Applicant's assertion. Buchanan in view of Datta does indeed teach the cited limitations. In further response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant argues (page 9 paragraph 4) that the cited portions of Buchanan et al. and Datta et al. fail to disclose a method wherein a second set of data entries identify provider edge routers corresponding to each of the customer edge routers, as recited in claim 5. However, Examiner respectfully disagrees with the Applicant's assertion. Buchanan teaches *a second set of data entries identifying provider edge routers* (service provider) *corresponding to each of the customer edge routers* (section 0035, Preferably when configuring VPNs, VPN tree 210 includes one or more of the following data categories: service provider, customers, sites (*customer edge routers*), site interfaces, VPNs, VPN components, VPN interfaces, and/or the like). Contrary to Applicant's remark that *a service provider data category disclosed in a VPN tree is not a set of data entries identifying provider edge routers corresponding to each of the customer edge routers, as set forth in claim 5*, Buchanan teaches (also see figure 2)

VPN tree having *provider edge routers* (service provider) *corresponding to each of the customer edge routers (*customers) and set of data (see figure 2, site 1, site 2, IF 1, IF 2 etc.).

35 USC 103 rejection of claims 3 and 4:

Claims 3 and 4 are not allowable for the same reasons.

35 USC 103 rejection of claim 7:

Applicant argues (page 11 paragraph 2) that the combination of Buchanan et at., Datta et al. and Chang et al. fails to disclose table entries that include the associated provider edge routes. However, Examiner respectfully disagrees with the Applicant's assertion. the combination of Buchanan et at., Datta et al. and Chang et al. do indeed teach the cited limitations. Specifically, Buchanan teaches d the table entries include the associated provider edge routes (section 0076, FIG. 4 shows an exemplary screen display of routing policy 400 for a site of the network of FIG. 1). Chang in the same field of endeavor teaches the rows are virtual private networks, a set of columns are defined by the customer edge routers (Figure 7). As such, Buchanan et at., Datta et al. and Chang et al. in combination do indeed teach the cited limitations. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claims 8-26:

Applicant has amended independent claims 8, 10 and 21. Applicant's amendment necessitated a new ground of rejections regarding claims 8-26 presented in this office action. As such any further response to Applicant's argument to said claims are moot.

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Salman Ahmed whose telephone number is (571) 272-8307. The examiner can normally be reached on 8:00 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SA
Salman Ahmed
Examiner
Art Unit 2619
2/12/2008

EDAN . ORGAD
SUPERVISORY PATENT EXAMINER